Modello di maturità della fiducia nei dati e nell'IA

Trovare la strada per un'IA sicura su larga scala

Trovare la strada per un'IA sicura su larga scala

Questo documento si basa su uno studio di ricerca indipendente condotto su 300 dirigenti aziendali e tecnologici nei settori dei servizi finanziari, sanità, governo, manifatturiero e tecnologia. I partecipanti includono dirigenti con responsabilità diretta su dati, sicurezza, rischio e strategia tecnologica. I risultati riflettono specificamente le risposte dei leader della C-suite di diversi settori, poiché sono loro i più vicini alle decisioni che determinano se l'IA potrà scalare in sicurezza o bloccarsi.

Esiste un notevole divario tra l'implementazione dell'IA e la prontezza a rispondere alle sue richieste. A livello globale, le aziende si classificano in livelli molto diversi di preparazione all'implementazione dell'intelligenza artificiale e a tutto ciò che essa comporta.

Il nostro report di ricerca sul modello di maturità della fiducia nei dati e nell'IA ha suddiviso le organizzazioni in cinque livelli, valutando la loro distribuzione, implementazione e preparazione. La nostra ricerca ha rilevato che il **95%** delle organizzazioni ha implementato l'IA nel proprio ambiente. Tuttavia, implementare l'IA in modo sicuro ed efficace si sta rivelando più difficile, perché le fondamenta operative necessarie per garantire fiducia nell'IA su larga scala richiedono più tempo per essere costruite rispetto all'adozione della tecnologia stessa.

L'AI sta scalando rapidamente, ma anche le battute d'arresto si moltiplicano

L'adozione dell'IA tra le organizzazioni di questi intervistati è già ben avviata. Quasi 7 su 10 affermano che l'intelligenza artificiale è già integrata in diverse funzioni aziendali o è fondamentale per le loro operazioni e la loro strategia competitiva. Eppure la stessa popolazione riferisce una serie di battute d'arresto difficili da conciliare con quel livello di maturità.

Circa il **52%** degli intervistati afferma che nel corso degli ultimi 18 mesi almeno un'iniziativa di IA è stata ridimensionata. 4 su 10 segnalano che le iniziative hanno subito ritardi rispetto alle tempistiche originarie. Più di 1 su 4 **(28%)** riporta un'iniziativa completamente interrotta, mentre circa 1 su 3 afferma che le proprie iniziative sono proseguite come previsto.

Queste difficoltà si verificano in organizzazioni in cui l'IA è già in produzione, il che significa che hanno meno a che fare con la fase iniziale di adozione e più con ciò che l'adozione richiede una volta raggiunta una diffusione su larga scala.

La velocità mette in luce le lacune

Gli ostacoli identificati dai leader aiutano a spiegare il perché. Il vincolo più frequentemente citato è la carenza di talenti nell'ambito dell'IA e del machine learning **(43%)**, seguita dalla difficoltà di integrare l'IA nei flussi di lavoro e nei sistemi esistenti **(33%)**. L'incertezza normativa **(25%)**, le limitazioni della qualità dei dati **(20%)** e le preoccupazioni relative alla spiegabilità **(19%)** aggiungono ulteriore pressione.

Queste sfide non sono indipendenti l'una dall'altra. Piuttosto, questi problemi si aggravano nelle organizzazioni che implementano rapidamente l'IA prima che la governance, le strutture di responsabilità e l'infrastruttura dati siano pronte a supportarla. La lista delle barriere, in questo senso, non è tanto un insieme di problemi distinti, bensì una descrizione di ciò che viene trascurato quando la velocità diventa la priorità.

In particolare, pochi dirigenti citano la tecnologia stessa come fattore limitante, a conferma del fatto che la maturità dell'IA è ora più vincolata dalla prontezza operativa che dalla velocità di innovazione.

Dove l'IA incontra dei limiti: Competenze, sistemi e standard

In apparenza, la fiducia dei dirigenti racconta una storia più ottimistica. Circa l'**80%** dei dirigenti afferma di essere fiducioso nella capacità della propria organizzazione di scalare l'IA in modo sicuro e responsabile nei prossimi due anni. La ricerca, tuttavia, rivela una distinzione cruciale: quasi la metà degli intervistati riconosce che la propria fiducia è guidata più dall'intuizione che da prove che potrebbero facilmente dimostrare a soggetti esterni. Tra i dirigenti la cui fiducia si fonda su un piano ben definito, tre fattori hanno quasi lo stesso peso:

55%

Un framework di governance formale

55%

Un impegno di leadership visibile

53%

Una funzione dedicata al rischio IA

Tuttavia, i numeri iniziano a diminuire quando si tratta di validazione esterna. Solo 31% dichiara di aver superato una revisione o un audit normativo che coinvolge l'IA, e appena **20%** fa riferimento al benchmarking rispetto ai pari del settore. Per la maggior parte delle organizzazioni, la fiducia si genera internamente piuttosto che essere verificata esternamente. Rispecchia i framework che i leader hanno progettato, i team che hanno costruito e le priorità che hanno definito — tutti elementi che devono essere messi alla prova esternamente per dimostrare di poter reggere in caso di emergenza.

Questa distinzione è importante man mano che le aspettative in materia di governance dell'IA si evolvono. Regolatori e consigli di amministrazione sono sempre meno interessati al fatto che la governance esista in linea di principio e sempre più focalizzati sulla possibilità di dimostrarla su richiesta.

Quasi 9 dirigenti su 10 affermano che esistono in qualche forma politiche formali di governance dell'IA. Eppure, solo circa uno su tre afferma di essere in grado di produrre immediatamente una documentazione di audit completa, se richiesto. Molti riconoscono che le prove esistono, ma la loro raccolta richiederebbe uno sforzo considerevole. Le politiche scritte e la governance verificabile sono capacità distinte e il divario tra di esse rappresenta una fonte significativa di esposizione al rischio.

I meccanismi di responsabilizzazione contribuiscono a consolidare questo schema. La maggior parte dei dirigenti attribuisce la responsabilità principale della governance dell'IA al CTO o al CDO, mentre una parte significativa si affida a comitati interfunzionali per coordinare la supervisione. Il **7%** dispone di un responsabile dedicato alla governance dell'IA.

Sebbene ciascuno di questi modelli possa essere efficace, dipendono da una chiara definizione di titolarità e responsabilità, due condizioni che diventano più difficili da mantenere man mano che l'IA si espande tra le funzioni. In assenza di ruoli espliciti e percorsi di escalation, la copertura delle policy non si traduce in modo affidabile in controllo operativo, soprattutto quando qualcosa va storto su larga scala.

La ricerca suggerisce un ambiente in cui l'adozione dell'IA è diffusa e l'ottimismo dei leader è elevato. Tuttavia, le basi operative necessarie per sostenere l'adozione e l'entusiasmo sono ancora in fase di definizione nella maggior parte delle organizzazioni. Le aziende che affrontano questa transizione in modo più efficace condividono una caratteristica distintiva: una fiducia fondata su prove tangibili. In particolare, le organizzazioni classificate ai livelli più alti di questo report (livelli quattro e cinque) tendono ad avere un programma di governance pratico, implementato e sottoposto a verifica, non solo progettato.

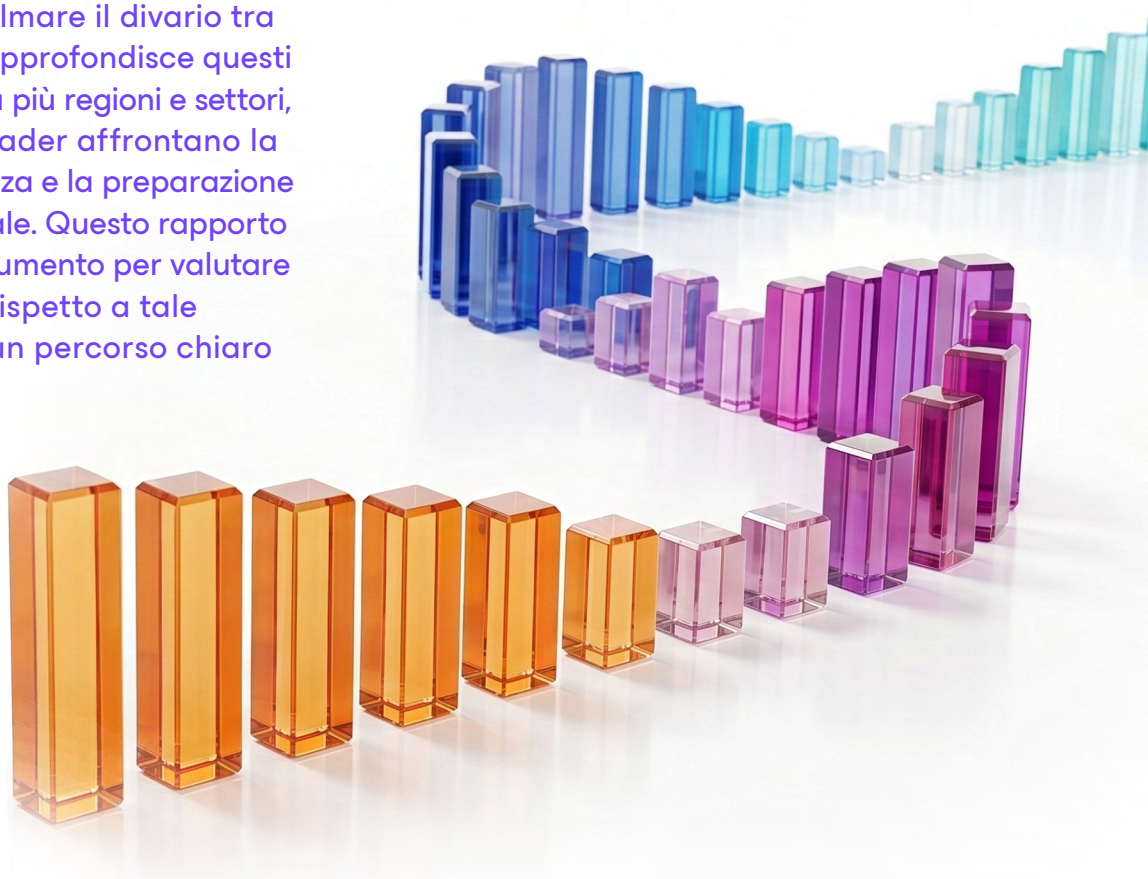
L'AI su larga scala premia la preparazione, non la rapidità

Il modello di maturità della fiducia nei dati e nell'IA offre ai leader un approccio strutturato e basato su benchmark per colmare il divario tra percezione e realtà. Valuta la coerenza con cui un'organizzazione governa, protegge, ripristina e abilita dati e intelligenza artificiale in tutta l'enterprise, misurando la realtà operativa piuttosto che le intenzioni dichiarate. Basato su ricerche e best practice, il modello misura cinque livelli di maturità, da ad hoc a leader di settore. Trasforma la prontezza da un'ipotesi in una capacità misurabile.

Per i leader che si chiedono se la loro fiducia sia superiore alle evidenze, offre anche il punto di riferimento esterno di cui la maggior parte delle organizzazioni è priva, secondo la ricerca.

Le organizzazioni con maggiori probabilità di sostenere l'IA su larga scala non sono necessariamente quelle che la adottano più rapidamente. Invece, sono coloro che investono precocemente nella governance, nella responsabilità e nelle basi dei dati che consentono all'IA di espandersi senza introdurre rischi che superino la loro capacità di gestirli.

Il report di ricerca completo sul modello di maturità della fiducia nei dati e nell'IA offre ai leader un approccio strutturato e basato su benchmark per colmare il divario tra percezione e realtà. approfondisce questi risultati estendendoli a più regioni e settori, ed esamina come i leader affrontano la governance, la resilienza e la preparazione all'intelligenza artificiale. Questo rapporto offre ai leader uno strumento per valutare la propria posizione rispetto a tale Standard e fornisce un percorso chiaro per raggiungerlo.



Metodi & Scopo

Questo executive summary si basa su una ricerca commissionata da Veeam condotta con 300 leader tecnologici e aziendali nei settori dei servizi finanziari, della sanità, della pubblica amministrazione, della produzione e della tecnologia. I rispondenti includevano dirigenti senior responsabili di dati, sicurezza, rischio e strategia tecnologica. I risultati citati in questo documento si concentrano sui rispondenti appartenenti alla C-suite all'interno della più ampia popolazione oggetto dello studio.

La ricerca ha esaminato come le organizzazioni stanno adottando, governando e scalando l'IA nella pratica, con particolare attenzione alla prontezza operativa, alle strutture di governance e alle condizioni che influenzano la fiducia della leadership. I risultati riflettono i comportamenti, gli esiti e le condizioni decisionali riportati, piuttosto che le intenzioni future dichiarate. I risultati di benchmark provengono dall'intero studio e rappresentano le risposte reali dei leader partecipanti, utilizzate per identificare i modelli comuni tra le organizzazioni man mano che l'IA passa dalla fase di implementazione iniziale all'integrazione nelle operazioni aziendali su larga scala.

Informazioni su Veeam Software

Veeam è l'azienda di fiducia per dati e IA, specializzata nell'aiutare le organizzazioni a garantire che i loro dati e la loro IA siano pienamente compresi, protetti e resilienti, al fine di accelerare l'adozione di un'IA sicura su larga scala. In qualità di leader di mercato nella resilienza dei dati e nella gestione della postura di sicurezza dei dati, Veeam è progettata per la convergenza di identità, dati, sicurezza e rischi legati all'intelligenza artificiale.

Veeam offre una profonda intelligenza contestuale su ogni asset di dati, identità e modello di intelligenza artificiale. L'azienda governa l'accesso sia per gli utenti sia per gli agenti IA, automatizza i processi di privacy, conformità e rimedio, protegge e ripristina le organizzazioni dalle minacce moderne, tra cui ransomware, disastri, errori dell'IA, e garantisce il ripristino di dati puliti e affidabili. Veeam consente alle organizzazioni di andare oltre la semplice protezione dei dati, permettendo loro di attivarne e sbloccarne tutto il potenziale.

Con sede a Seattle e uffici dislocati in oltre 30 Paesi, Veeam protegge oltre 550.000 clienti in tutto il mondo, tra cui l'82% delle aziende Fortune 500, che si affidano a Veeam per mantenere operative le proprie attività.

Per saperne di più, è possibile visitare www.veeam.com o seguire Veeam su LinkedIn @veeam-software e X @veeam.